Unsealed 6/29/23 MS

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

FILED
JUN 13 2023
US DISTRICT COURT
DISTRICT OF DELAWARE

SEALED

UNITED STATES DISTRICT COURT

for the

District of Delaware

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The premises known as [redacted]

Case No. 23- 265M

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-1, incorporated herein.

located in the _____ District of Delaware, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2252A(a)(1)	Transportation of Child Pornography
18 USC 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Randy Mullins
Applicant's signature

Randy Mullins, Special Agent, United States Air Force
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: June 13, 2023

Judge's signature

City and state: Wilmington, DE

The Honorable Jennifer L. Hall, U.S. Magistrate Judge
Printed name and title

SEALED

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

IN THE MATTER OF THE SEARCH OF 1) [redacted] 2) Paul Michael Wilcox 3) Wilcox's vehicles: 2017 Dodge Durango, License Plate: [redacted] VIN: [redacted] and 2022 Dodge Charger, License Plate: [redacted] VIN: [redacted]

Case No. 23- 265M

Filed Under Seal

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Randy Mullins, a Special Agent with the United States Air Force Office of Special Investigation ("OSI"), Dover, Delaware, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as [redacted] (the "SUBJECT PREMISES"), the person of Paul Michael Wilcox ("WILCOX"), and his registered vehicles: a 2017 Dodge Durango, License Plate: [redacted] VIN: [redacted] and a 2022 Dodge Charger, License Plate: [redacted] VIN: [redacted] both registered to the SUBJECT PREMISES (together, the "SUBJECT LOCATIONS"), more fully described in Attachments A-1, A-2, and A-3, for the things described in Attachment B. Attachments A and B are incorporated herein by reference.

2. I am a Special Agent ("SA") with OSI and a credentialed federal agent authorized to investigate violations of the Uniform Code of Military Justice, as well as violations of State and Federal laws where a military nexus exists. I have served with OSI since September 2016 and as

a Special Agent since January 2019. I am a graduate of the Federal Law Enforcement Training Center's Criminal Investigator Training Program, the United States Air Force Special Investigations Academy, the Sex Crimes Investigations Training Program, and the National Criminal Justice Training Center Undercover Concepts and Techniques. I graduated from the Community College of the Air Force in 2019, where I received an associate degree in Criminal Justice. Since joining OSI, I have served in multiple capacities as a Special Agent and have completed tours as a field level Special Agent, protective service officer, counterintelligence Special Agent, and have served in various supervisory roles.

3. I currently assist the Delaware Internet Crimes Against Children Task Force (the "Delaware ICAC") with investigations where a military nexus exists. The primary goal of the Delaware ICAC will be to expand the quantity and quality of detection, investigation, apprehension, and prosecution of electronic communications-facilitated crimes against children.

4. I have experience in numerous investigative disciplines to include child exploitation, child sexual abuse, various adult sex crimes, cyber-based investigations, financial crimes, narcotics investigations, fraud, and espionage. I have received substantial training related to child exploitation, narcotics trafficking, online undercover operations, interviewing techniques, surveillance and counter-surveillance techniques, and multiple other criminal investigator-related facets.

5. As a federal agent, I am authorized to investigate violations of laws of the United States, including Title 18, United States Code, Sections 2252A(a)(1) and 2252A(a)(5)(B), and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

6. The statements contained in this affidavit are based in part on information and reports provided by U.S. federal law enforcement agents and state law enforcement officers; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals, and my experience, training, and background as a Special Agent. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish that there is sufficient probable cause for the requested warrant.

7. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that device(s) located within the SUBJECT PREMISES or devices operated by WILCOX uploaded child pornography to the Google account [redacted] ("TARGET ACCOUNT"). Specifically, a device connected to the home internet at the SUBJECT PREMISES accessed the TARGET ACCOUNT which contained child pornography. Such actions violate Title 18, United States Code, Section 2252A(a)(1) (Transportation of Child Pornography) and Title 18, United States Code, Section 2252A(a)(5)(B) (Possession of Child Pornography) (hereinafter, the "SPECIFIED FEDERAL OFFENSES"). There is also probable cause to search the information described in Attachments A-1, A-2, and A-3 for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachments B.

SPECIFIED FEDERAL OFFENSES

8. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2252A(a)(1) prohibits a person from

knowingly mailing, transporting, or shipping any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer.

b. Title 18, United States Code, Sections 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

9. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

c. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

d. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image

of picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. "Cloud-based storage service," as used herein, refers to a publicly accessible, online storage provider that collectors of depictions of minors engaged in sexually explicit conduct can use to store and trade depictions of minors engaged in sexually explicit conduct in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders or collectors of depictions of minors engaged in sexually explicit conduct in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an Internet connection.

f. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, tablets, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

g. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

h. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible

or unusable, as well as reverse the process to restore it.

i. "Data," as used herein refers to the quantities, characters, or symbols on which operations are performed by a computer, being stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media.

j. "Digital Devices" as used herein refers to any physical object that has a computer, microcomputer, or hardware that is capable of receiving, storing, possessing or potentially sending data.

k. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. A "hash value" (or "hash ID") is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

m. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

n. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

o. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

p. "Mobile applications," as used herein, are small, specialized programs

downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

q. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

r. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

s. "Cloud storage" is an online central storage location that allows users to access their files from anywhere using a device connected to the Internet.

t. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

u. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

v. "User Attributes," as used herein refers to any tangible data, documents, settings, programs or other information that provides information related to the identity of the specific user of the device, computer, application, program or record.

w. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO POSSESS AND COLLECT CHILD PORNOGRAPHY, AND HOW USE OF COMPUTERS AND THE INTERNET RELATES TO THE POSSESSION, RECEIPT AND/OR DISTRIBUTION OF CHILD PORNOGRAPHY

10. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who utilize the Internet to view and transport images of child pornography are often individuals who have a sexual interest in children and in images of children,

and that there are certain characteristics common to such individuals, including the following:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or cellphone, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer to Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images.

Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

11. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers, smartphones and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers, smartphones and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Mobile devices such as laptop computers, smartphones, iPods, iPads and digital media storage devices are known to be used and stored in vehicles, on persons or other areas outside of the residence.

d. Smartphones have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smartphone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smartphone can also easily plug the device into a computer, via a USB cable, and transfer data files from one digital device to another. Many people generally carry their smartphone on their person.

e. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to

another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography.

f. Child pornography can be transferred via electronic mail or through file transfer protocols ("FTP") to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

g. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo, and Google, Inc., Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is maintained on the servers of the providers and is occasionally retained by the providers after the user deletes the data from their account.

h. A "hash value" is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

i. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

j. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and the increased storage capacity of computers and server space over time, there exists a fair probability that evidence regarding the distribution, receipt, and possession of child pornography will be found in the SUBJECT PREMISES notwithstanding the passage of time.

k. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.

l. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten.

m. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.

n. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over 2 TB of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

o. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Since the storage capacity of hard drives has increased dramatically over the last several years, it is more likely that the above-described information will be recovered during forensic analysis.

BACKGROUND CONCERNING GOOGLE[1]

12. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google

[1] The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

13. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

14. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

15. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

16. Gmail is an Internet-based electronic communications system operated by Google. It permits its users to communicate using e-mail through their Gmail service, instant messages, text messages, and group messages through their Hangouts and Voice[2] services, and other social networking type methods.

17. Google integrates its various services to make it easier for Google Accounts to access the

[2] Google Voice provides a phone number for calling, text messaging, and voicemail. It works on smartphones and computers, and syncs across devices. According to Google, Calls, text messages, and voicemails are stored and backed up.

full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

18. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

19. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers

or other devices were used to access the Google Account.

PROBABLE CAUSE

20. On or about May 30, 2023, OSI received a cybertip from the National Center for Missing & Exploited Children ("NCMEC"). NCMEC's CyberTipline is the nation's centralized reporting system for the online exploitation of children. The public and electronic service providers can make reports of suspected online enticement of children for sexual acts, child sexual molestation, child sexual abuse material, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the internet. This cybertip was initiated by Google and reported that the Google account [redacted] ("the Google Account") uploaded 64 files, 28 of which Google categorized as containing or displaying apparent child pornography.

21. Google provided both the IP address information for the file uploads, as well as the phone number associated with the Google Account. Based upon the IP address location and the phone number, it was ascertained that the violations likely occurred in Delaware and were likely associated with Air Force Chief Master Sergeant Paul Michael Wilcox ("WILCOX"), who was stationed at Dover Air Force Base at the time of the cybertip. The phone number associated with the Google Account is the same phone number the Air Force has on file for WILCOX. Additionally, WILCOX provided the same phone number to the Dover Air Force Base Middle School in February 2022 for an incident involving his daughter.

22. On or about June 2, 2023, your affiant obtained a federal search warrant to view the files from the cybertip, issued by the Honorable Christopher J. Burke, U.S. Magistrate Judge for the District of Delaware. The search warrant authorized law enforcement to view the 64 files uploaded

by the Google Account, that Google supplied to law enforcement in their cybertip.

23. On or about June 5, 2023, your affiant and law enforcement officers from the Delaware ICAC viewed the files from the cybertip originating from the Google Account. Examples of some of the files are described as follows:

a. report_7567007714137504 86.jpg – Image depicted a prepubescent white female laying on a bed on a presumed male's legs appearing to being penetrated by the male's penis. The breasts and top of the vagina were visible.

b. report_1252333379389055422.png – Image depicted a white female, estimated approximately 8 years old with apparent male ejaculation on her face. The tip of a penis was barely visible at the bottom of the picture.

c. report_2369779341270528433.png – Image depicted a prepubescent female of Asian descent, estimated age approximately 6 years old, fully nude, sitting on top a white male. The male's penis was penetrating the female child's vagina.

d. report_3870828806190082816.jpg – Image depicted a white female, photographed from behind, on her hands and knees. Her vagina and anus are visible. The photo was taken from between the legs of an apparent adult male. His penis was visible in the photo. Difficult to determine age of white female but likely a child less than 12 years old.

e. report_6536119414713383384.jpg – Image depicted a prepubescent white female, estimated age approximately 6 years old, standing fully nude, holding the penis of a fully nude adult male. The adult male had his arm around the female child. The female child's chest and vagina were visible.

f. report_7351389843237274243.jpg – Image depicted a prepubescent white female, fully nude, with her head laying on the stomach of a naked male. The male's penis appeared

to touch the female child's lips and nose. It was difficult to determine the age of the male but he could possibly be another child.

g. report_9034799750365650241.jpg – Image depicted a prepubescent white female, estimated age approximately 6 years old, laying on her stomach between the legs of an apparent adult male. She was licking the penis of the adult male. She wore a t-shirt and appeared to wear no pants or underwear; however, none of her genitalia was visible.

24. On or about May 31, 2023, a subpoena was served on Google. Google responded with information that the account was created on March 9, 2023.

25. In the cybertip, Google reported the following IP address associated to the Google Account upload: 2600:4040:716f:1900:8165:d644:37bc:914a (Login) 05/10/2023 10:01:24 UTC. A check of publicly available records determined that the IP address was assigned to Verizon Communications Corporation ("Verizon"). On or about May 31, 2023, a subpoena was served on Verizon for subscriber information associated to the IP address.

26. A response from Verizon provided that the subscriber assigned to the IP address is Paul Wilcox, with a listed address of the SUBJECT PREMISES; listed phone number as that associated with the Google Account in the cybertip, and verified as belonging to WILCOX; and e-mail address of [redacted]. Verizon further provided that the account was created on November 3, 2021. Air Force records show that WILCOX moved to Dover Air Force Base on November 1, 2021, which is two days before the Verizon account was opened. WILCOX lives at the SUBJECT PREMISES with his wife and two minor children, ages 13 and 14.

SUMMARY

27. In summary, based on the facts above, there is probable cause to believe that WILCOX uploaded child pornography to the Google Account in violation of the SPECIFIED FEDERAL

OFFENSES. First, the phone number associated with the Google Account is the same phone number the Air Force has on file for WILCOX and is the same phone number WILCOX provided to his daughter's school in February 2022. Second, the user of the Google Account accessed the account and completed the upload while connected to the internet at the SUBJECT PREMISES, i.e. WILCOX's residence. Moreover, the Google Account was recently created on March 9, 2023 – approximately two months before the upload of child pornography. The Google Account uses the name [redacted] WILCOX lives at the SUBJECT PREMISES with his wife and two minor children, none of whom are named any variation of [redacted] In fact, an Internet search for the term [redacted] yields a business called "Jenray Products," one such product being a moonshine scented air freshener. Additionally, the Google Account is tied to WILCOX's phone number, not his wife's. Given the creation date and name, as well as my training and experience, there is reason to believe the Google Account was created for the purpose of anonymizing illicit activity pertaining to the SPECIFIED FEDERAL OFFENSES. In light of all the above, there is probable cause to believe that WILCOX is the user of the Google Account and that he uploaded child pornography to the Google Account.

28. There is also probable cause to believe that contraband, evidence, fruits, and instrumentalities of violations of the SPECIFIED FEDERAL OFFENSES will be found in the SUBJECT LOCATIONS. First, as discussed above, there is probable cause to believe that WILCOX transported and possessed child pornography and used a digital device to do so using the Google Account. Thus, based on my training and experience, WILCOX has a sexual interest in children as described in paragraphs 10 and 11, *supra*.

29. Second, based on my training and experience and as described above in paragraph 10, *supra*, individuals who have a sexual interest in children not only tend to collect and distribute

child pornography, but tend to use multiple devices to view, collect, and send child pornography. They also not only use devices from their place of residence, they sometimes leave their devices in their residence. This is especially true if such individuals believe they will imminently be searched by law enforcement. Further, computer files or remnants of such files can be recovered months after they have been viewed via the Internet, downloaded onto a storage medium, or even deleted. Therefore, there is probable cause to believe that WILCOX is in possession of at least one device that contains evidence, fruits, and instrumentalities of, and contraband related to the sexual exploitation of children in violation of the SPECIFIED FEDERAL OFFENSES. This warrant seeks authorization to search for and seize all such devices identified as belonging to WILCOX, as more fully described in Attachment B.

30. Information connected to the devices used to access the Google Account may also provide indirect evidence of the offenses under investigation, such as Internet searches indicative of an interest in children, e-mails or application downloads indicating membership in forums on the dark web that are known to be dedicated to the sexual exploitation of children, specific user attributes, or original media indicative of producing child pornography.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

31. As described above and in Attachment B, this application seeks permission to search for contraband, evidence, fruits, and instrumentalities of violations of the SPECIFIED FEDERAL OFFENSES that might be found at the SUBJECT LOCATIONS, in whatever form they are found. One form in which the evidence might be found is as records in the form of data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure and search of computers and storage media and, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

32. *Probable cause:* I submit that if a computer or storage medium is found within the SUBJECT LOCATIONS, there is probable cause to believe that records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

33. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer or storage medium in the SUBJECT LOCATIONS because:

e. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

f. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further

suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information

described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

j. I know that when an individual uses a computer to access with intent to view, possess, distribute, or receive child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

34. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

k. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As

explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

l. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

m. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

35. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B) and in compliance with circuit and district search procedures/protocols, the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by

the warrant.

BIOMETRIC ACCESS TO DEVICES

36. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through their fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through their face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of their face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with their irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers their irises by holding the device in front of their face. The device then directs an infrared light toward the user's face and activates an infrared-

sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, certain Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of WILCOX to the fingerprint scanner of the devices found at the PREMISES; (2) hold the devices found at the PREMISES in front of the face of WILCOX and activate the facial recognition feature; and/or (3) hold the devices found at the PREMISES in front of the face of WILCOX and activate the iris recognition feature, for the purpose of attempting to

unlock the devices in order to search the contents as authorized by this warrant.[3] The proposed warrant does not authorize law enforcement to compel that WILCOX state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to compel WILCOX to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

[3] "[I]dentifying physical characteristic[s]" are not testimonial and thus fall "outside [the] protection" of the Fifth Amendment. *Gilbert v. California*, 388 U.S. 263, 266-67 (1967). The privilege against self-incrimination, therefore, is not violated by an order compelling a person to submit to photographing and measurements or to provide fingerprints, writing samples, or voice exemplars. *See, e.g.*, *United States v. Dionisio*, 410 U.S. 1, 7 (1973); *California v. Byers*, 402 U.S. 424, 431-32 (1971); *Gilbert*, 388 U.S. at 266-67; and *Schmerber v. California*, 384 U.S. 757, 763-64 & n.8 (1966). Thus, compelling an individual to place a finger or thumb on the Touch ID of an electronic device does not implicate the Fifth Amendment for the same reasons. *See In the Matter of the Search Warrant Application for [Redacted Text]*, 279 F. Supp. 3d 800, 800-06 (N.D. Ill. 2017) (holding that the compelled act of placing finger on device was not an act of communication and therefore not testimonial pursuant to the Fifth Amendment); *Matter of Search of [Redacted] Washington District of Columbia*, 317 F. Supp. 3d 523 (D. D.C. June 26, 2018) (same); *Matter of White Google Pixel 3 XL Cellphone in a Black Incipio Case*, 2019 WL 3401990 (D. Idaho July 26, 2019) (same); *Minnesota v. Diamond*, 890 N.W.2d 143, 151 (Minn. Ct. App. 2017) (same); *Virginia v. Baust*, No. CR 14-1439, 2014 WL 10355635 (Va. Cir. Ct. Oct. 28, 2014) (same); *see also United States v. Sanudo-Duarte*, No. CR-14-01342-002-PHX-JAT, 2016 WL 126283 (D. Ariz. Jan. 12, 2016) (holding that defendant could be compelled to provide exemplar of his palm prints since they were not testimonial); *United States v. Warrant*, 2019 WL 4047615, (N.D. Cal. Aug. 26, 2019) (same).

CONCLUSION

37. Based on the foregoing information, I submit there is probable cause to believe that contraband, evidence, fruits, and instrumentalities of violations of the SPECIFIED FEDERAL OFFENSES as set forth herein and in Attachment B are currently contained within the SUBJECT LOCATIONS, more fully described in Attachments A-1, A-2, and A-3. I therefore respectfully request that a search warrant be issued authorizing a search of the SUBJECT LOCATIONS for the items described above and in Attachment B, and authorizing the seizure and examination of any such items found therein.

Respectfully submitted,

/s/ Randy Mullins
Special Agent Randy Mullins
Air Force Office of Special Investigations

Sworn to me over the telephone and signed by me pursuant to
Fed. R. Crim. P. 4.1 on this 13 day of June, 2023

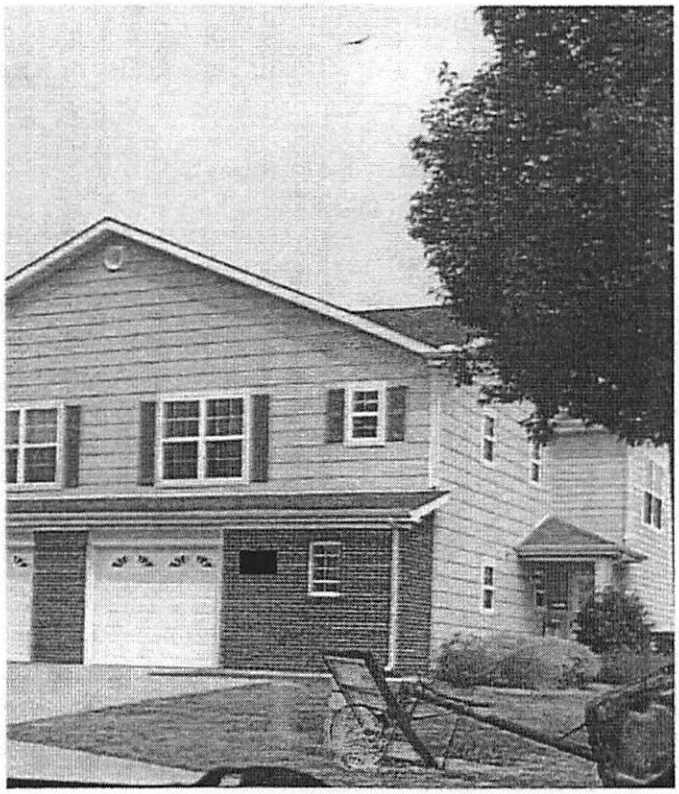
Honorable Jennifer L. Hall
United States Magistrate Judge

ATTACHMENT A-1

PROPERTY TO BE SEARCHED

The residence known as [redacted] (the "SUBJECT PREMISES). The residence is a two-story duplex home, with a tan colored roof, light blue and brick exterior, and a shared private driveway leading to a single car garage. The numbers [redacted] are clearly marked in black lettering on a white background attached to the brick on the front of the residence. The main door in located to the right side of the residence when facing the residence from Hemlock street. Below is an image of the residence that Affiant captured on June 8, 2023:

(Source: surveillance by affiant on/about June 8, 2023)

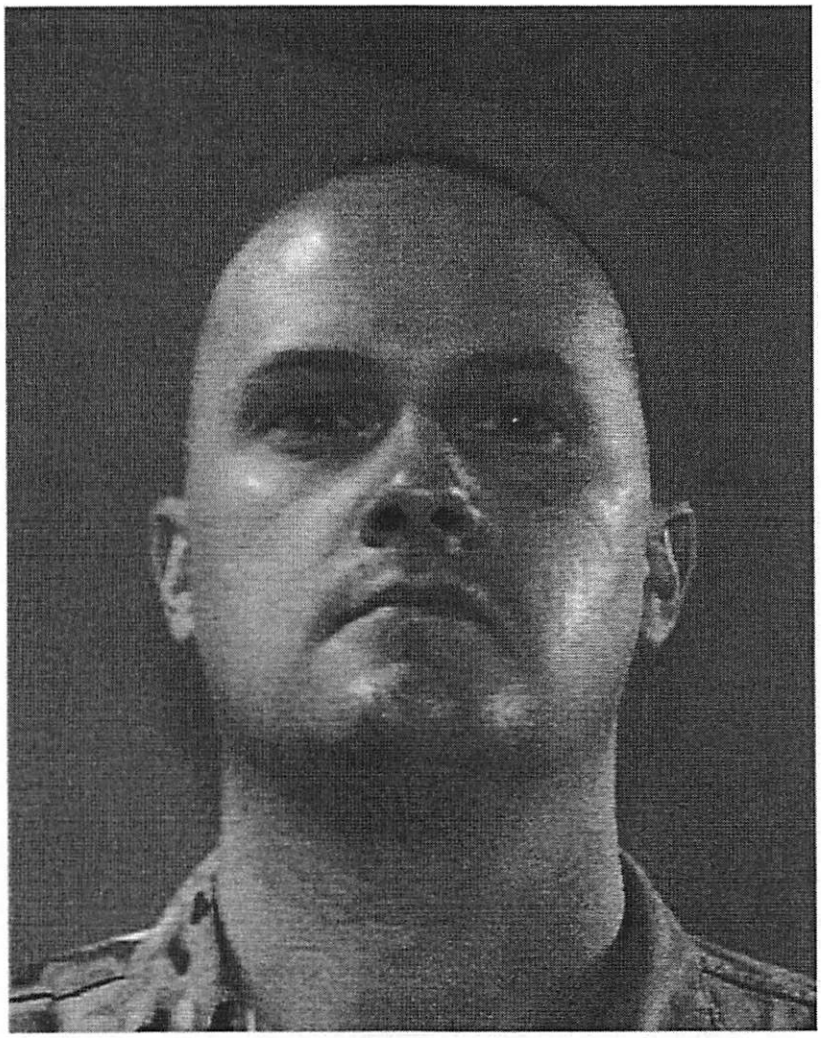


ATTACHMENT A-2

PERSON TO BE SEARCHED

The person to be searched is Paul WILCOX, DOB: [redacted], SSN: [redacted]

WILCOX is a Caucasian male approximately six feet in height and weighs approximately 175 pounds. OSI reviewed several photographs of WILCOX via social media and military databases. Below is a photo of WILCOX taken from Air Force Databases.



ATTACHMENT A-3

VEHICLES TO BE SEARCHED

1. 2017 Gray Dodge Durango, License Plate: [redacted] VIN: [redacted]. This vehicle is registered to WILCOX at the SUBJECT PREMISES.

2. 2022 Orange Dodge Charger, License Plate: [redacted], VIN: [redacted]. This vehicle is registered to WILCOX at the SUBJECT PREMISES.

ATTACHMENT B

PROPERTY TO BE SEIZED

The following materials which constitute contraband, evidence, fruits, or instrumentalities of Title 18, United States Code, Section 2252A(a)(1) (Transportation of Child Pornography) and Title 18, United States Code, Section 2252A(a)(5)(B) (Possession of Child Pornography) (hereinafter, the "SPECIFIED FEDERAL OFFENSES"):

1. All COMPUTERS and STORAGE MEDIA (as defined below) located in the SUBJECT LOCATIONS identified as belonging to WILCOX, including:

   a. Those found on WILCOX's person;
   b. Those found in WILCOX's vehicles;
   c. Those found in WILCOX's bedroom, sleeping quarters, or home office;
   d. Those found within close proximity to WILCOX's person at time of encounter; and
   e. Those identified by a resident of the SUBJECT PREMISES as belonging to WILCOX.

2. For the COMPUTERS and STORAGE MEDIA (hereinafter, "DEVICES"):

   a. evidence of who used, owned, or controlled the DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
   b. evidence of software that would allow others to control the DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
   c. evidence of the lack of such malicious software;
   d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
   e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;
   f. evidence of the attachment to the DEVICES of other storage devices or similar containers for electronic evidence;
   g. evidence of programs (and associated data) that are designed to eliminate data from the DEVICES;
   h. evidence of the times the DEVICES were used;

i. passwords, encryption keys, and other access devices that may be necessary to access the DEVICES that are found stored within the DEVICES;
j. documentation and manuals that may be necessary to access the DEVICES or to conduct a forensic examination of the DEVICES;
k. records of or information about Internet Protocol addresses used by the DEVICES;
l. records of or information about the DEVICES' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
m. contextual information necessary to understand the evidence described in this attachment;
n. any and all adapters, chargers, or other hardware items necessary to charge the battery, or to maintain the functioning of, the DEVICES;
o. records and information relating to the sexual exploitation of children, including files, correspondence, and/or communications about or stored on the Instagram account;
p. records and information showing access to and/or use of the Instagram account;
q. records and information relating or pertaining to the identity of the person or persons using or associated with the Instagram account; and
r. child pornography and child erotica.

3. Records, information, and items relating to violations of the SPECIFIED FEDERAL OFFENSES, including:

a. records, information, and items relating to WILCOX's occupancy of the SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;
b. records, information, and items relating to the ownership or use of the DEVICES, including sales receipts, bills for Internet access, and handwritten notes;
c. records and information relating to the identity or location of the persons suspected of violating the statutes described above; and
d. Child pornography and child erotica in any form.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

This warrant authorizes a review of computer and storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, law enforcement may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

During the execution of the search of the Subject Premises described in Attachments A-1, A-2, and A-3, law enforcement personnel are authorized to press or swipe the fingers (including thumbs) of WILCOX to the fingerprint scanner of the devices found at the SUBJECT LOCATIONS; (2) hold the devices found at the SUBJECT LOCATIONS in front of the face of WILCOX and activate the facial recognition feature; and/or (3) hold the devices found at the SUBJECT LOCATIONS in front of the face of WILCOX and activate the iris recognition feature,

for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.